U.S. General Services Administration (GSA)

PRESIDENTIAL TRANSITION “HOT ISSUES” INFORMATION PAPER

SUBJECT: Security Enhancement

1. BACKGROUND:

GSA’s Security Enhancement includes support for the on-going Cybersecurity National Action Plan (CNAP) High Value Asset (HVA) Assessments, which are designed to enhance cybersecurity awareness and protections, safeguard privacy, and maintain public safety as well as economic and national security.

In addition, GSA’s Office of the Chief Information Officer (GSA IT) is also providing support for other on-going security assessments, particularly the development of the Low-Impact Authority to Operate (ATO) process for Software as a Service (SaaS). Offices within GSA have identified many new SaaS products that they would like to utilize, but believe that the currently process for granting an ATO to these services is onerous, costly, and slow. Therefore, GSA IT is working to determine the best way to ATO these SaaS products for our own environment, with hopes that the process can be studied and leveraged by FedRAMP and other agencies.

a. General Background:

- The Department of Homeland Security (DHS), as the operating entity responsible for HVA Assessments at all Federal civilian agencies, is conducting penetration testing on top 3 GSA HVAs
- GSA is facilitating and supporting HVA assessments
- GSA is responsible for remediating the findings of GSA’s 3 HVA Assessments
- GSA is creating a stream-lined Low Impact ATO process for SaaS vendors
- Low Impact process can be used by FedRAMP program

b. Issues:

- Of the 3 systems being assessed, GSA does not totally own the systems (they are supported, in whole or in part) through vendors, so testing and remediation for these systems is a highly sensitive matter
- One GSA HVA vendor is awaiting new contract
- Obtaining Government-wide acceptance of Low-Impact SaaS ATO process

2. SCOPE AND EFFECT:

a. Impact on GSA’s Customers:

- The HVA assessments will ensure GSA customers that the GSA IT systems they are using are secure
- The Low-Impact SaaS ATO process will allow GSA to provide products and services to GSA customers more quickly

b. Impact on the Private Sector and State & Local Governments:

- HVA assessments may have a financial impact depending on what the findings are and how much they will cost to remediate
- Impact on key stakeholders for the Low Impact SaaS initiative is to reduce time and money for SaaS implementations. This would also help improve partnership with the private sector in understanding and meeting federal security requirements. The Low Impact SaaS initiative and assessments can be shared with State and Local governments.
- Exact time and money reductions for Low Impact SaaS deployment will be calculated once the issue achieves initial operating capability (IOC).

3. ACTION(S) PLANNED OR REQUIRED:

Initial HVA assessments are expected to be completed and findings are to reported over the next few months. Once DHS issues the HVA report, GSA will work with the vendors to ensure that all findings are remediated in an effective and efficient manner in order to ensure the security of Federal Government data and systems. An exact plan of action will be determined when DHS delivers the assessment reports. GSA IT will then review and plan remediation activities, including any additional funds or capabilities that may be needed to successful address any DHS recommendations.

Once the Low Impact SaaS ATO process is completed, GSA will test out the new process on a few SaaS vendors as part of the IOC. Once IOC is complete and the greater government-wide community (including FedRAMP) approves of the new process, it will be rolled out across government (as part of FedRAMP) for full operating capability (FOC).

4. KEY STAKEHOLDER INTEREST:

Key stakeholders for the HVA assessment project include GSA, DHS, the Office of Management and Budget (OMB), and the vendor community that is being assessed. All parties have an interest in ensuring the HVA assessments are completed and that any findings are remediated in an effective and efficient way to ensure the Federal Government's data remains secure.

5. FISCAL YEAR 2017/2018 BUDGET IMPACT:

Currently, there are no budget impacts or issues related to the security initiatives noted above.